UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,622	03/30/2004	Kazumasa Omote	1924.70199	3471

7590 10/30/2008

Patrick G. Burns, Esq.
GREER, BURNS & CRAIN, LTD.
Suite 2500
300 South Wacker Dr.
Chicago, IL 60606

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
10/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/812,622	OMOTE ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-6,8,11,13,15-19,22-25,27,28,34,35 and 41-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,8,11,13,15-19,22-25,27,28,34,35,41-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application amendments filed on **7-10-2008**.

2. Claims **1, 3 - 6, 8, 11, 13, 15 - 19, 22 - 25, 27, 28, 34, 35, 41 - 43** are pending. Claims **1, 3 - 6, 8, 11, 13, 15 - 19, 22 - 25, 27, 28, 34, 35** have been amended. Claims **2, 7, 9, 10, 12, 14, 20, 21, 26, 29 - 33, 36 - 40** have been cancelled. Claims **41 - 43** are new. Claims **1, 3, 5, 6, 8, 11, 13, 15, 16, 18, 19, 22, 23, 24, 25, 27, 28, 34, 35** are independent. This application was filed on **3-20-2004**.

Response to Arguments

3. Applicant's arguments filed 7-10-2008 have been fully considered but they were not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose, "changing the setting information upon it being judged at the judging that the communication is executed by the worm. (see Remarks Page 27); "changing the judgment criteria upon it being judged at the judging unit that the communications is executed by the worm". (see Remarks Page 27)

The Spiegel prior art discloses that the parameters are adjustable and can be changed or weighted based on another parameters. The parameters are changeable. (see Spiegel col. 5, lines 15-21: dynamic (i.e. adjustable, changeable) parameters for worm determination; relative (percentage) parameters used; col. 5, lines 47-53: heuristic can be fine tuned)

The Willebeek-LeMair discloses self-hardening of the detection system. (Willebeek-LeMair paragraph [0054], lines 1-14: tuning operation performed in an automated manner; paragraph [0055], lines 1-17: effectuates a self-hardening system; paragraph [0056], lines 1-16: threat detection and threat suppression (firewall) capabilities of the system are continually being optimized (by the interlocking and agent functionalities to response to continuous threat assessment analysis)

3.2 Applicant argues that the referenced prior art does not disclose, the threshold criteria are based on historical data for failed connection attempts". (see Remarks Page 28)

There is no disclosure in the specification or the original claims for the usage of historical data. The term "historical" is not disclosed in the specification or the original claims. Spiegel discloses the usage of historical data. (see Spiegel (see Spiegel col. 3, lines 58-67: worm determination; col. 5, lines 8-15: history or recorded information utilized in worm determination)

3.3 Applicant argues that the referenced prior art does not disclose, "judgment that a communications is executed by a worm. (see Remarks Page 27-30)

Siegel discloses a determination that communications is executed by a worm. Spiegel and its combination with Willebeek-LeMair and Bunker disclose the criteria of a large number of packets used to make the determination of a worm and additional criteria. (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses and information not matching criteria for

normal traffic setting; col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

3.4 Applicant argues that the referenced prior art does not disclose, predicting a type of the worm. (see Remarks Page 31)

The Willebeek-LeMair prior art discloses the usage of detection signature that can be used by other systems to determine the type of attack. (see Willebeek-LeMair paragraph [0030], lines 1-17: digital signature; determination type of attack (worm))

3.5 Claims 41 - 43 are new claims. Arguments concerning these claims will not be addressed.

3.6 The Spiegel prior art discloses retrieving reference information for a communications packet. (see Spiegel col. 4, lines 17-20; col. 4, lines 27-31; col. 4, lines 45-48: calculation address accesses in worm determination) In addition, the Spiegel and Willebeek-LeMair prior art combination discloses the specific extraction of reference information from a communications packet. (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number)) And, the Spiegel and Willebeek-LeMair prior art combination discloses blocking a communication packet(s) from entrance to a protected (internal) network segment from an external (outside) network segment. (see Willebeek-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph [0035], lines 7-14: block communications packets between network segments (inside network segment and outside network segment))

The Spiegel prior art discloses a software, computer program implementation of the prior art invention. A software implementation implies program module to operate as functional units performing specific functions such as extracting information utilizing an extraction unit and judging criteria utilizing a judging unit. (see Spiegel col. 6, lines 15-24: module (functional unit(s)) design for software implementation)

Claim Rejections - 35 USC § 101

4. The 101 rejection has been withdrawn.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims **1, 3 - 6, 8, 11, 13, 16 - 19, 22 - 24, 34, 41 - 43** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Spiegel et al.** (US Patent No. **7,159,149**) in view of **Willebeek-LeMair et al.** (US PGPUB No. **20030204632**).

Regarding Claims 1, 13, Spiegel discloses a computer readable recording medium for storing a computer program, device for detecting a worm by monitoring a

communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

a) acquiring information related to a traffic and a communication address of a communication packet based on setting information; (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses and information not matching criteria for normal traffic setting; col. 2, lines 51-53; col. 2, lines 62-65; col. 6, lines 15-22: software, implementation means;) and

b) judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria; (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

e) changing the setting information upon it being judged at the judging that the communication is executed by the worm; wherein the acquiring includes acquiring the information based on the setting information after a change. (see Spiegel col. 5, lines 15-21: dynamic (i.e. adjustable, changeable) parameters for worm determination; col. 5, lines 47-53: heuristic can be fine tuned; col. 6, lines 15-22: software, implementation means)

Spiegel does not specifically disclose extracting reference information for identifying a communication packet, and blocking the communication packet as part of worm determination.

However, Willebeek-LeMair discloses:

c) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number)) and

d) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting. (see Willebeck-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph [0035], lines 7-14: block communications packets between network segments (inside network segment and outside network segment))

It would have been obvious to one of ordinary skill in the art to modify Spiegel to block network access after a determination of a worm has been judged as taught by Willebeek-LeMair. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11: "... *Self-deployed security defense is achieved by having the included defense functionalities work together to automate threat detection and threat response operations. Self-hardening security defense is achieved by having the included functionalities implement threat detection and threat response operations in an optimized manner*

that mitigates instances of false detection. ... ")

Regarding Claims 3, 16, Spiegel discloses a computer-readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information;

(see Claim 1: a, b, c, d for rejection)

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

(see Claim 1: a, b, c, d for rejection)

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm;

(see Claim 1: a, b, c, d for rejection)

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

(see Claim 1: a, b, c, d for rejection)

changing the judgment criteria upon it being judged at the judging that the communication is executed by the worm, wherein the judging includes judging whether the communication is executed by the worm based on the information acquired and the setting information after change. (see Spiegel col. 5, lines 8-10; col. 5, lines 15-21: worm determination based on information and adjusted (i.e. changed) information; col. 6, lines 15-22: software, implementation means)

Regarding Claims 4, 17, Spiegel discloses the computer readable recording medium, device according to claims 1, 15, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm when there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 3, lines 20-27: network communication packets throughput increased, worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claims 5, 18, Spiegel discloses a computer-readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a

communication packet based on setting information;

(see Claim 1: a, b, c, d for rejection)

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

(see Claim 1: a, b, c, d for rejection)

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm;

(see Claim 1: a, b, c, d for rejection)

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

(see Claim 1: a, b, c, d for rejection)

f) a communication from a computer in the predetermined network segment is judged previously to be executed by the worm, (see Spiegel col. 5, lines 8-10: history of worm detection; col. 5, lines 47-50: particular source/destination addresses (i.e. for a computer) monitored; col. 6, lines 15-22: software, implementation means) and

g) the number of destination addresses of the communication packet that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of a communication packet

acquired when the communication is judged to be executed by the worm, and is transmitted from the predetermined network segment to the outside. (see Spiegel col. 3, lines 20-27: worm determination based on number of packets transferred to addresses (i.e. inside or outside local network); connection attempts (destination addresses))

Regarding Claims 6, 19, Spiegel discloses a computer-readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information;

(see Claim 1: a, b, c, d for rejection)

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

(see Claim 1: a, b, c, d for rejection)

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm;

(see Claim 1: a, b, c, d for rejection)

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

(see Claim 1: a, b, c, d for rejection)

e) there is an increase in number of responding communication packets corresponding to communication packets that are transmitted from outside to the predetermined network segment, (see Spiegel col. 4, lines 17-22: communications increase (i.e. inside or outside local network), worm determination; col. 6, lines 15-22: software, implementation means) and

f) there is an increase in number of sender addresses of the communication packets. (see Spiegel col. 3, lines 20-27: communications (i.e. address, and process port number) increases, worm determination; sender addresses (connection attempts))

Regarding Claim 8, Spiegel discloses a computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information;

(see Claim 1: a, b, c, d for rejection)

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

(see Claim 1: a, b, c, d for rejection)

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm;

(see Claim 1: a, b, c, d for rejection)

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

(see Claim 1: a, b, c, d, e for rejection)

wherein the judging includes predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that is recorded in advance. (see Spiegel col. 3, lines 58-67: worm determination; col. 5, lines 8-15: history or recorded information utilized in worm determination; col. 6, lines 15-22: software, implementation means)

Regarding Claim 11, Spiegel discloses a computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to

perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information;

(see Claim 1: a, b, c, d for rejection)

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

(see Claim 1: a, b, c, d for rejection)

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm;

(see Claim 1: a, b, c, d for rejection)

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

(see Claim 1: a, b, c, d, e for rejection)

cutting off includes cutting off the communication executed by the worm by stopping a process that is started by the worm. (see Spiegel col. 2, lines 13-18: terminate affected process (i.e. stopping a process), worm determination; col. 6, lines 15-22: software, implementation means)

wherein the cutting off includes cutting off the communication executed by the worm by making a fire wall function effective in a computer that is judged to have a

worm. (see Spiegel col. 6, lines 48-55: firewall functioning; col. 6, lines 15-22: software, implementation means)

Regarding Claims 22, 23, 24, 34, Spiegel discloses a computer-readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information;

(see Claim 1: a, b, c, d for rejection)

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

(see Claim 1: a, b, c, d for rejection)

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm;

(see Claim 1: a, b, c, d for rejection)

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

(see Claim 1: a, b, c, d, e for rejection)

Spiegel does not specifically disclose extracting a port number. However, Willebeek-LeMair discloses wherein the extracting includes extracting as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging. (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number))

It would have been obvious to one of ordinary skill in the art to modify Spiegel for extracting a port number in determination of a worm as taught by Willebeek-LeMair. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

Regarding Claim 41, Spiegel discloses the computer-readable recording medium according to claim 3, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm based on communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 1, lines 50-62: connections attempts (communication packets) directed to a destination address used in determination of a worm) Spiegel

does not specifically disclose an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted. However, Willebeek-LeMair discloses wherein an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted. (Willebeek-LeMair paragraph [0007], lines 8-12: large numbers of packets and connection requests (destination address))

It would have been obvious to one of ordinary skill in the art to modify Spiegel for an increase in number of communication packets as well as number of destination addresses of communication packets as taught by Willebeek-LeMair. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

Regarding Claim 42, Spiegel discloses the computer-readable recording medium according to claim 6, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm based on communication packets as well as a number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 1, lines 50-62: connections attempts (communication packets) directed to a destination address used in determination of a worm) Spiegel does not specifically disclose an increase in number of communication packets as well

as number of destination addresses of communication packets that are transmitted. However, Willebeek-LeMair discloses wherein an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted. (Willebeek-LeMair paragraph [0007], lines 8-12: large numbers of packets and connection requests (destination address))

It would have been obvious to one of ordinary skill in the art to modify Spiegel for an increase in number of communication packets as well as number of destination addresses of communication packets as taught by Willebeek-LeMair. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

Regarding Claim 43, Spiegel discloses the computer-readable recording medium according to claim 8, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm based on communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 1, lines 50-62: connections attempts (communication packets) directed to a destination address used in determination of a worm) Spiegel does not specifically disclose an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted.

However, Willebeek-LeMair discloses wherein an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted. (Willebeek-LeMair paragraph [0007], lines 8-12: large numbers of packets and connection requests (destination address))

It would have been obvious to one of ordinary skill in the art to modify Spiegel for an increase in number of communication packets as well as number of destination addresses of communication packets as taught by Willebeek-LeMair. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair in order to enable the capability to threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

7. Claims **25, 27, 28, 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Spiegel-Willebeek-LeMair** and further in view of **Bunker et al.** (US PGPUB No. **20030056116**).

Regarding Claims 25, 27, 28, 35, Spiegel discloses the computer program, computer-readable medium, method, device according to claims 1, 12, 13, 14, 33. (see Spiegel col. 1, lines 48-62: monitoring for worm determination; col. 4, lines 45-48: traffic analysis, calculation utilizing network addressing (IP address, port number)) a computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is

connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information;

(see Claim 1: a, b, c, d for rejection)

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria;

(see Claim 1: a, b, c, d for rejection)

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm;

(see Claim 1: a, b, c, d for rejection)

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

(see Claim 1: a, b, c, d for rejection)

Spiegel does not specifically disclose calculations utilizing reference information such as port numbers in the analysis of work determination. However, Bunker discloses wherein the extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the

worm at the judging, and extracting, as the reference information, a type of the communication wherein the number of the communication packets is over a threshold value. (see Bunker paragraph [0189], lines 1-11; paragraph [0215], lines 1-5; paragraph [0220], lines 8-12: calculation (summation) of access information in worm determination)

It would have been obvious to one of ordinary skill in the art to modify Spiegel to calculate a summation of reference information utilized for worm determination as taught by Bunker. One of ordinary skill in the art would have been motivated to employ the teachings of Bunker in order to enable the capability to emulate hacker methodology in a safe way and enable study of network security openings without affecting customer operations. (see Bunker paragraph [0012], lines 1-8: "*... To answer the security needs of the market, a preferred embodiment was developed. A preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions. External vulnerability assessment tests can emulate hacker methodology in a safe way and enable study of a network for security openings, thereby gaining a true view of risk level without affecting customer operations. ...*")

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
October 14, 2008